STATE OF ALABAMA

Information Technology Policy

Policy 660-03: Application Security Testing

The application testing process is vital in identifying security flaws before the application is released, but testing the security of an application differs from standard testing. Instead of verifying the application performs a function as intended, the tester needs to attempt to get the application to perform unauthorized and undocumented functions. This often involves attempting to make an application function fail and then exploiting the failure to compromise the application or the system it is running on.

OBJECTIVE:
Identify and correct application security flaws.

SCOPE:
This policy applies to all application designers, developers, testers and their managers; to all applications deployed or in development including (but not necessarily limited to) client-server applications, Web-based applications, database applications; and to all application and system components including test platforms and application source code.

RESPONSIBILITIES:
Organizations are required to test applications for security flaws before the application is deployed, before modifications are released, and periodically throughout the life of the application. Specific roles/responsibilities for conducting security testing are as follows:

Test Team Manager or Program Manager:

Ensure at least one tester has been designated to test for security flaws.

Ensure test procedures are created, documented, and periodically executed.

Ensure testers are provided periodic training, on at least an annual basis, allowing them to efficiently and thoroughly test the application for security flaws.

Ensure code coverage statistics (the percentage of the application code exercised during the testing process) are maintained within the testing documentation for each application.

Ensure a security-focused code review is performed before the application is released.

Ensure reviewers are objective parties holding no responsibilities for developing the application being tested.

Code reviews may be automated or manual. The most comprehensive reviews will implement two or all of the following review types.

- Automated Code Review
- Manual Code Review
- Third Party Code Review

Automated code reviews may be the only feasible option to review code for an entire application; however automated review tools often return false positives and may fail to identify some categories of security vulnerability. Document and utilize code review procedures that address disqualifying false positives and manually checking for security vulnerabilities test tools fail to identify.

Testers:

Security flaws often occur in areas of the code not regularly executed, so ensure all code is covered during application testing.

Ensure the application does not contain code never invoked during operation.

Ensure the application does not modify data files outside the scope of the application.

Ensure all test machines are compliant with system security policies.

Ensure the system remains in a secure state during system initialization, shutdown, and aborts.

Managers, Designers, Developers, and Testers:

Prepare misuse cases. A use case defines how an application should behave. A misuse case is the opposite of a use case; its sole purpose is to identify how an application should not behave. Misuse cases help testers prepare test cases purely to test the security strength of the system. A misuse case should capture the type of attacks that can be made on the system and how the system should behave in such situations.

Remove any residual backup files, temporary files, File Transfer Protocol programs, debugging files, tools, accounts, passwords, debug and test flags, and other unnecessary files and developer "backdoors" from the application code and its underlying host environment prior to release.

Actively monitor application security developments as new classes of vulnerabilities are continuously being discovered.

ENFORCEMENT:
Refer to Information Technology Policy 600-00: Information Security.
http://isd.alabama.gov/policy/Policy_600-00_Information_Security.pdf

ADDITIONAL INFORMATION:
DEFINITIONS: Refer to Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Signed by Jim Burns, Chief Information Officer

DOCUMENT HISTORY:

Version	Release Date	Comments
Original	6/4/2008	